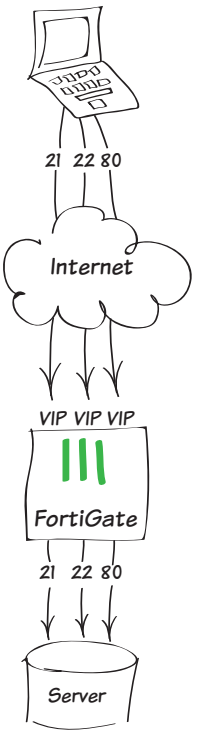
Using port forwarding to allow limited access to an internal server

This example illustrates how to use virtual IPs to configure port forwarding on a FortiGate unit. In this example, TCP ports 80 (HTTP), 21 (FTP), and 22 (SSH) are opened, allowing remote connections to communicate with a server behind the firewall.

1. Creating three virtual IPs
2. Adding the virtual IPs to a VIP group
3. Creating a security policy
4. Results

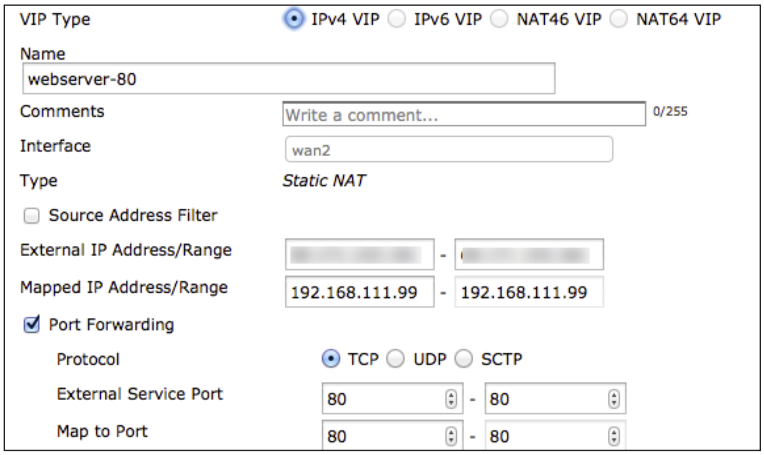


1. Creating three virtual IPs

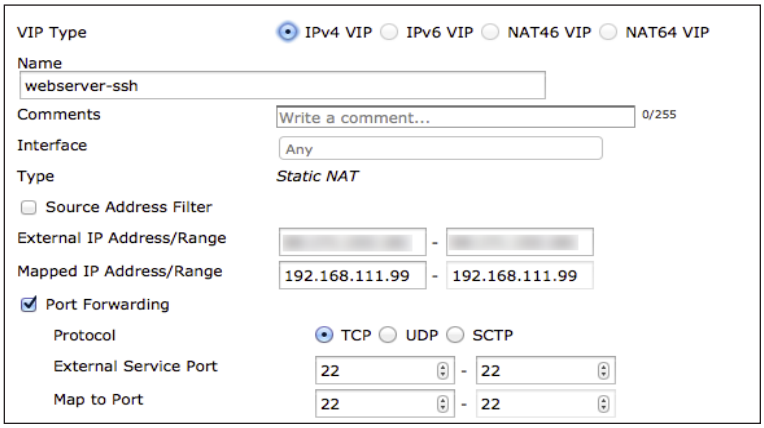
Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP.**

Enable **Port Forwarding** and add a virtual IP for TCP port 80. Label this VIP *webserver-80*.

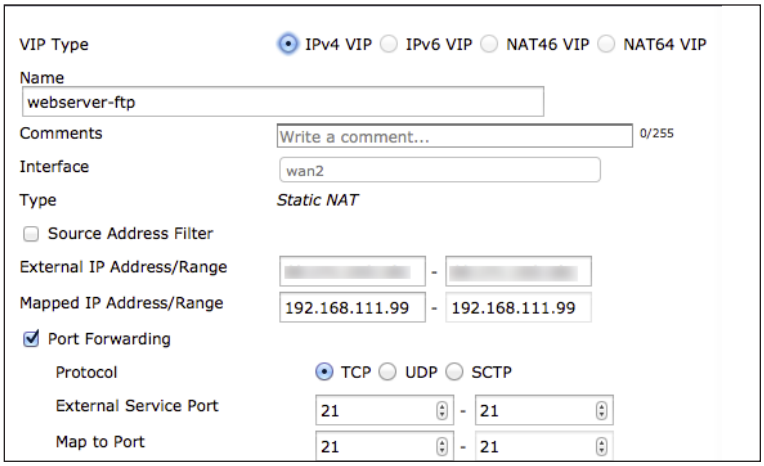
While this example maps port 80 to port 80, any valid External Service port can be mapped to any listening port on the destination computer.



Create a second virtual IP for TCP port 22. Label this VIP *webserver-ssh*.



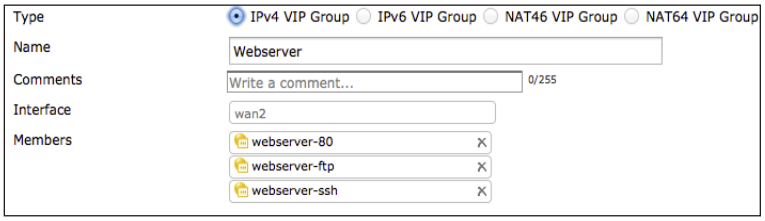
Create a third a virtual IP for TCP port 21. Label this VIP *webserver-ftp*.



2. Adding virtual IPs to a VIP group

Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP Group.**

Create a VIP group. Under **Members,** include all three virtual IPs previously created.

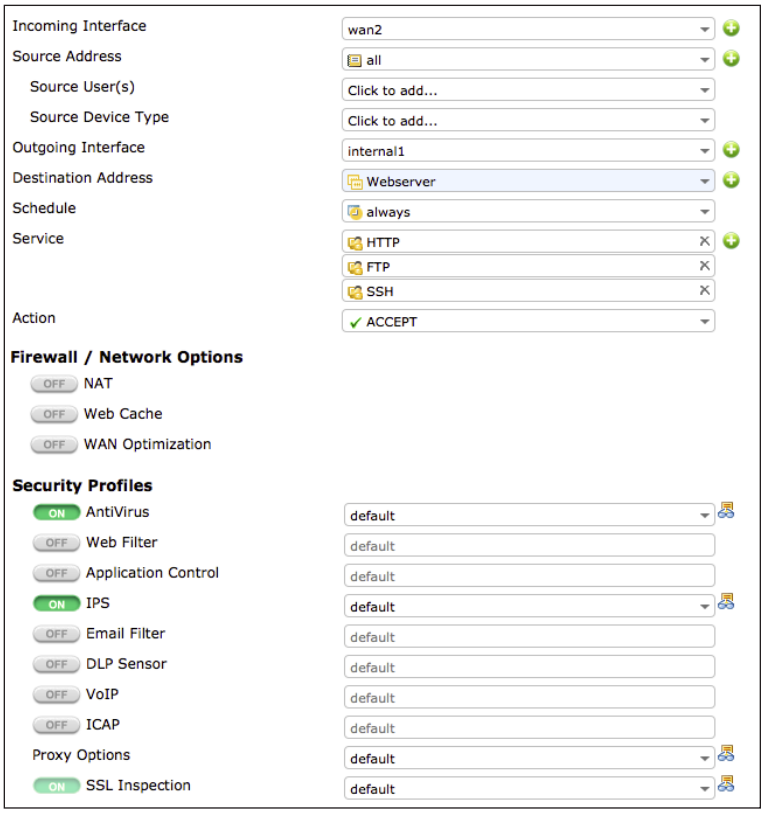


3. Creating a security policy

Go to **Policy & Objects > Policy > IPv4** and create a security policy allowing access to a server behind the firewall.

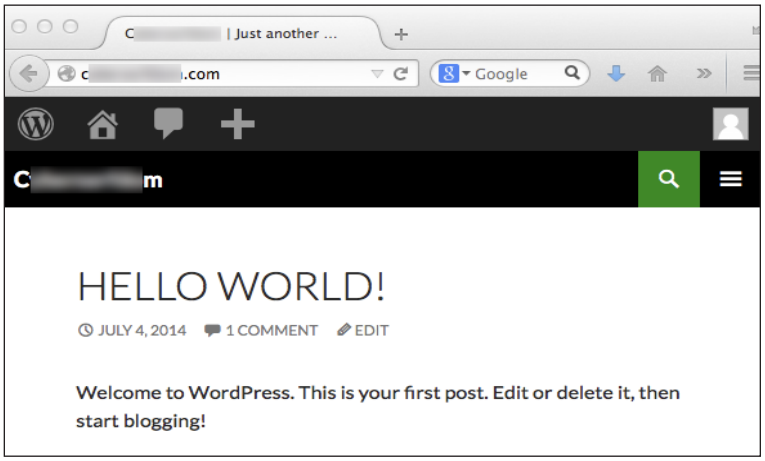
Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination** address to the VIP group. Set **Service** to allow **HTTP**, **FTP**, and **SSH** traffic.

Use the appropriate **Security Profiles** to protect the servers.

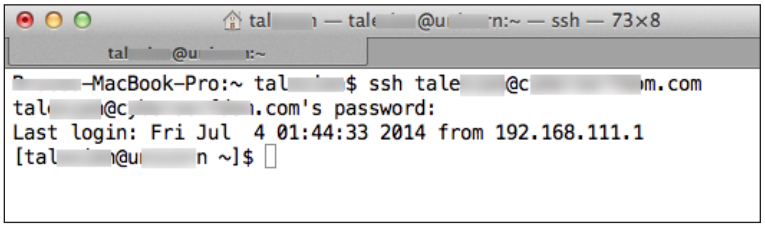


4. Results

To ensure that TCP port 80 is open, connect to the web server on the other side of the firewall.



To ensure that TCP port 22 is open, connect to the SSH server on the other side of the firewall.



To ensure that TCP port 21 is open, use an FTP client to connect to the FTP server on the other side of the firewall.